UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/938,790	08/24/2001	Alexander I. Alten	Alten-00100	2157

7590 06/16/2006

Richard Butler
Valley Oak Law
5655 Silver Creek Valley Rd # 106
San Jose, CA 95138

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 06/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/938,790	**Applicant(s)** ALTEN, ALEXANDER I.	
	Examiner Zachary A. Davis	**Art Unit** 2137	

-- Th MAILING DATE of this communication appears on th cov r sh t with th correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *13-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *13-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. A response to the Notice of Non-Compliant Amendment (mailed 17 March 2006) was received on 13 April 2006. By this response, Claims 13, 14, and 16-23 have been amended. Previously withdrawn Claims 1-12 and 24-29 have been canceled. No new claims have been added. Claims 13-23 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 12 January 2006 have been fully considered but they are not persuasive.

Claims 13, 16, 19, and 21 were rejected under 35 U.S.C. 103(a) as being unpatentable over Koopman, Jr., US Patent 5696828, in view of Wilson et al, US Patent 5295188. Claims 14, 15, and 20 were rejected under 35 U.S.C. 103(a) as being unpatentable over Koopman in view of Wilson, and further in view of Ritter, US Patent 5623549. Claims 17, 18, 22, and 23 were rejected under 35 U.S.C. 103(a) as being unpatentable over Koopman in view of Wilson, and further in view of Schneier, *Applied Cryptography*.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208

USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Specifically, regarding independent Claims 13 and 19, Applicant alleges that Koopman teaches away from the claimed invention by teaching the use of a unique, non-repeating, and independently varying value such as date and time (see pages 10-11 of the present response, citing Koopman, column 7, lines 22-33) and not a random value. The Examiner respectfully disagrees that this statement teaches away from the claimed invention. First, the Examiner notes that this step of performing an exclusive OR (Koopman, column 7, lines 22-33) occurs after the first step of shuffling (column 5, line 60-column 6, line 22, noting particularly column 6, lines 12-15), to which the argument primarily appears directed, noting that the values that are shuffled are sampled directly from the source of random data and are therefore, in fact, random (see column 4, line 59-column 5, line 51, detailing the chaotic noise source and the processes of sampling and further insuring randomness of the data). The Examiner further notes that even if the above were not the case, combining such a non-repeating value as described by Koopman (column 7, lines 22-33) with a truly random value (as generated by the chaotic noise source of Koopman, column 4, line 59-column 5, line 51) would still result in a random value. That is, combination with another, not necessarily random, number does not de-randomize the random number.

Applicant further argues that Koopman does not teach nested shuffling of a plurality of large random secrets as claimed (see page 10 of the present response). However, as noted in the previous Office action, the Koopman was not relied upon for the explicit teaching of a nested shuffle; instead, the Wilson reference was relied on to teach a nested shuffle for generating keys.

Applicant further alleges that Wilson fails to teach nested shuffling each of a plurality of large random secrets, etc., as recited in Claims 13 and 19 (see page 11 of the present response). However, this argument fails to comply with 37 CFR 1.111(b) because it amounts to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Further, as noted above, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Specification

3. The objection to the disclosure for informalities is withdrawn in light of the amendments to the specification. The Examiner again notes that the lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Objections

4. The objection to Claims 16 and 21 for informalities is withdrawn in light of the amendments to the claims.

5. Applicant is advised that should claims 13, 14, and 16-18 be found allowable, claims 19-23 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k). The Examiner notes that it appears that Claim 19 is intended to read "A method for deciphering a sequence of cipher text" in place of "A method for enciphering a sequence of cipher text". The objection would be overcome if such a change were made.

Claim Rejections - 35 USC § 112

6. The rejection of Claims 13-23 under 35 U.S.C. 112, second paragraph, as indefinite, is withdrawn in light of the amendments to the claims.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 13, 16, 19, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koopman, Jr., US Patent 5696828, in view of Wilson et al, US Patent 5295188.

In reference to Claim 13, Koopman discloses a method for enciphering that includes shuffling a plurality of large random secrets using a plurality of mixing keys (column 5, line 60-column 6, line 22), performing an XOR to produce a plurality of pads (column 7, lines 22-33), rotating the values of the plurality of pads (column 8, lines 18-34, noting the use of a shift register), shuffling a portion of the rotated pads (column 5, line 60-column 6, line 22), performing an XOR to produce a final pad (column 7, lines 22-33), selecting a portion of the final pad to form a key stream (column 7, lines 46-49, where portions of the random numbers are eliminated), and performing an XOR on the key stream and clear text values (column 1, lines 51-58, noting that the generated random numbers are used as a key for a Vernam stream cipher). However, Koopman does not explicitly disclose that the first shuffle is a nested shuffle.

Wilson discloses that random sequences can be used to generate cryptographic keys (column 5, lines 24-30), and that for greater security, shuffling of key material can be done at multiple levels (column 9, lines 26-31, where a global shuffle and a local shuffle can be performed). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Koopman by including a nested shuffle, in order to increase security (see Wilson, column 9, lines 26-29) and provide verifiable random number sequences (see Wilson, column 2, lines 66-68).

Claim 19 is directed to a method of deciphering cipher text that corresponds to the enciphering method of Claim 13, and is rejected by a similar rationale.

In reference to Claims 16 and 21, Koopman and Wilson further disclose selecting a series of portions to form the key stream (Koopman, column 7, lines 46-49).

9. Claims 14, 15, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koopman in view of Wilson as applied to claims 13 and 19 above, and further in view of Ritter, US Patent 5623549.

Koopman and Wilson disclose everything as applied above to Claims 13 and 19; however, neither Koopman nor Wilson explicitly discloses substituting values within the plurality of secrets. Ritter discloses a cipher method that includes initializing mechanisms by substituting values within tables for other values within the tables (column 18, lines 13-18). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the methods of Koopman and Wilson to include the substitution of Ritter, in order to increase the strength of the ciphering (see Ritter, column 5, line 67-column 6, line 2).

10. Claims 17, 18, 22, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koopman in view of Wilson as applied to claims 13 and 19 above, and further in view of Schneier, *Applied Cryptography.*

In reference to Claims 17 and 22, Koopman and Wilson disclose everything as applied to Claims 13 and 19 above. Koopman and Wilson further disclose the use of a secure channel for distributing keys (Wilson, column 1, lines 44-47). However, neither Koopman nor Wilson explicitly discloses the use of a central server to distribute keying information. Schneier discloses that a central trusted server can be used to generate and distribute key information (page 47, "Key Exchange with Symmetric Cryptography", noting the Key Distribution Center). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the methods of Koopman and Wilson by including a Key Distribution Center, in order to gain the security of the trusted secure server (see Schneier, page 47, last paragraph).

In reference to Claims 18 and 23, Koopman and Wilson disclose everything as applied to Claims 13 and 19 above. Koopman and Wilson further disclose the use of a secure channel for distributing keys (Wilson, column 1, lines 44-47). However, neither Koopman nor Wilson explicitly discloses the use of a storage medium to distribute keying information. Schneier discloses that the large amounts of key bits for a one-time pad can be distributed on a CD or digital tape (see the paragraph spanning pages 16-17). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the methods of Koopman and Wilson by including distribution of keying information on a storage medium, in order to allow for easy storage and access to the large number of key bits required for a Vernam stream cipher, i.e. one time pad (see Schneier, paragraph spanning pages 16-17).

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER